

УДК 004.75

И.А. Трещёв

Оценка временных затрат для осуществления распределенного перебора в гетерогенных системах при помощи временных волновых систем

Рассматривается метод получения априорной верхней и нижней оценок временных затрат на осуществление распределенного перебора в гетерогенных системах при помощи временных волновых систем. Приведены временные оценки для различных вариантов построения гетерогенных систем.

Ключевые слова: распределенный перебор, оценка временных затрат.

Для задач защиты информации актуальной является проблема распределенного перебора в неоднородных (гетерогенных) системах. Пусть область перебора вариантов D , например для задачи отыскания неприводимого многочлена над заданным полем [1], состоит из векторов $\bar{x} = (x_1, x_2, \dots, x_n)$, если данную область можно представить в виде объединения непересекающихся подобластей, то представляется возможным применение методики распределенного перебора. Данная методика заключается в распределении непересекающихся подобластей исходной области D между различными вычислительными узлами так, чтобы свести обмены информацией между узлами к минимуму, наилучший вариант – к нулю. Довольно часто при реализации распределенного перебора используют парадигму «один ведущий, много ведомых» [2].

Одной из формальных математических моделей для организации распределенного перебора и оценки временных затрат на его исполнение является модель временных волновых систем [4]. Данная модель вполне адекватно описывает вычислительный процесс для неоднородных сред за счет введения времени исполнения каждой операции, выполняемой в процессе вычислений, и времени передачи данных по коммуникационной среде.

Например, в настоящее время в сети Internet существует проект по распределенному перебору всех чисел Мерсена, но до сих пор не ясно, сколько времени будет потрачено в рамках данного проекта для оценки простоты очередного числа. В связи с этим актуальной является проблема оценки времени исполнения некоторого вычислительного процесса для распределенных, разнородных, объединенных вычислительных узлов, таких как компьютеры в сети Internet.

Теоретические сведения

Рассмотрим гетерогенную вычислительную систему, состоящую из различных вычислительных узлов (со стандартными процессорами, устройствами хранения данных, блоками питания и т.д.), подключенных к сети (локальной или глобальной) при помощи стандартных протоколов передачи информации, например Ethernet, Fast Ethernet, Gigabit Ethernet.

Для каждого вычислительного узла заданы его производительность (количество операций с плавающей точкой в секунду) и время выполнения простых операций (сложение, вычитание, умножение, деление и т.д.) на нем. Для сети и используемых в ней протоколов заданы параметры передачи информации (пропускная способность, латентность, которая складывается из программной и аппаратной задержек), причем сеть – однородна в том смысле, что все узлы передают данные друг другу по одному и тому же протоколу. Размеры передаваемых между вычислительными узлами блоков данных одинаковы. Пусть для рассматриваемой вычислительной системы латентность на прием данных не совпадает с латентностью на передачу данных.

Определение. Моделью волновой системы или просто волновой системой [3] будем называть простой ациклический частичный орграф

$$G = (A, V, dom, cod),$$

у которого для каждой вершины $v \in V$, её прообразы $dom^{-1}(v)$, $cod^{-1}(v)$, если они определены, являются конечными линейноупорядоченными множествами. Предполагается, что в состав волновой системы включено отношение порядка, обозначаемое символом $<$.

Под временной волновой системой понимается волновая система, для которой определены пара вещественных чисел $\bar{\tau} \geq 0$ и $\tau \geq 0$, и функция $t:V \rightarrow R$ во множество вещественных чисел, принимающая неотрицательные значения. Числа $\bar{\tau} \geq 0$ и $\tau \geq 0$ интерпретируются как время записи в канал и чтения из канала, связывающего два вычислительных узла. Значения $t(v)$ – время выполнения операции, соответствующей вершине частичного орграфа.

Вершинам орграфа временной волновой системы можно поставить в соответствие вычислительные узлы гетерогенной системы, которые выполняют различные операции по ребрам связи между ними. Функция t будет определять время исполнения вычислений для каждой из вершин, числа $\bar{\tau}$ и τ в сумме определяют время передачи данных между вычислительными узлами.

В работе [4] было показано, что для временной волновой системы время её функционирования не превышает времени функционирования всех вершин и времени передачи данных по всем ребрам:

$$\sum_{v \in V} t(v) + |A|(\tau + \bar{\tau}) \geq T_{AWS} \geq d(\max_{l \in \text{Trace}_{AWS}}(l)).$$

Величину $\sum_{v \in V} t(v) + |A|(\tau + \bar{\tau})$ назовем верхней оценкой времени работы данной временной волновой системы и обозначим $T_{AWS}^{\max}$, а $d(\max_{l \in \text{Trace}_{AWS}}(l))$ – нижней оценкой и обозначим $T_{AWS}^{\min}$.

Определим AWS^* – множество всевозможных волновых систем. Определим отношение равенства на множестве AWS^* следующим образом:

$\forall AWS_1, AWS_2 \in AWS^* \quad AWS_1 = AWS_2$ тогда и только тогда, когда $A_1 = A_2$, $V_1 = V_2$, $dom_1 = dom_2$, $cod_1 = cod_2$.

Параллельная композиция

Определим операцию «+» параллельной композиции для двух волновых систем следующим образом:

Пусть $AWS = (A, V, dom, cod)$, $AWS' = (A', V', dom', cod')$, тогда $AWS + AWS' = AWS_+$, в случае, если $A \cap A' = \emptyset$, $V \cap V' = \emptyset$. $AWS_+ = (A \cup A', V \cup V', dom \cup dom', cod \cup cod')$.

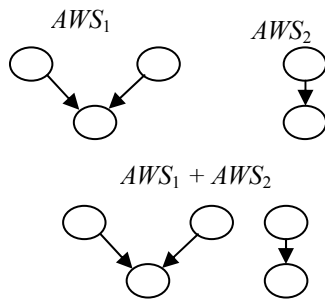


Рис. 1. Пример параллельной композиции двух волновых систем

Утверждение 1. Операция «+» – коммутативна и ассоциативна.

Доказательство:

1) Коммутативность: Докажем, что $AWS + AWS' = AWS' + AWS = AWS_+$, $AWS + AWS' = AWS_+$, $AWS_+ = (A \cup A', V \cup V', dom \cup dom', cod \cup cod')$, $AWS' + AWS = AS$, $AS = (A' \cup A, V' \cup V, dom' \cup dom, cod' \cup cod)$, $AWS_+ = AS$ (это следует из коммутативности объединения).

2) Ассоциативность: $AWS_1 + (AWS_2 + AWS_3) = (AWS_1 + AWS_2) + AWS_3 = AWS'$. Доказательство аналогично предыдущему и следует из ассоциативности объединения.

Обозначим AWS_0 – волновую систему, у которой множество A пусто, множество V пусто, множество dom пусто и множество cod пусто: $AWS_0 = (\emptyset, \emptyset, \emptyset, \emptyset)$. $AWS_0 \in AWS^*$ (по определению AWS^*).

Утверждение 2. $(AWS^*, +)$ – коммутативная полугруппа.

Доказательство: по определению $\forall AWS_1, AWS_2, AWS_1 + AWS_2 \in AWS^*$ и операция «+» коммутативна и ассоциативна (Утверждение 1).

В дальнейшем AWS_0 будем называть пустой волновой системой. Как видно из рис. 1, параллельная композиция волновых систем соответствует независимому их выполнению.

Утверждение 3. $(AWS^*, +)$ – коммутативный моноид.

Доказательство:

Необходимость: единицей этого моноида является пустая волновая система. Нетрудно убедиться в том, что $\forall AWS \in AWS^* \quad AWS + AWS_0 = AWS_0 + AWS = AWS$.

Достаточность: докажем от противного. Предположим, что $\exists AWS' \neq AWS_0$, такая, что $\forall AWS \in AWS^*$ имеет место $AWS + AWS' = AWS' + AWS = AWS$. По определению $AWS + AWS' = (A \cup A', V \cup V', dom \cup dom', cod \cup cod')$. $AWS + AWS' = AWS_+ = AWS$, $AWS_+ = (A \cup A', V \cup V', dom \cup dom', cod \cup cod')$, отсюда следует $A \cup A' = A$, $V \cup V' = V$, $dom \cup dom' = dom$, $cod \cup cod' = cod$, откуда заключаем, что $A' = \emptyset$, $V' = \emptyset$,

$dom'=\emptyset, cod'=\emptyset$ – противоречие, т.е. $AWS'=AWS_0$, а значит, пара $(AWS^*, +)$ – коммутативный моноид (единица единственна).

Утверждение 4. $(AWS^*, +)$ – не группа.

Доказательство: пусть $\forall AWS' \in AWS^*$, такой, что $AWS' \neq AWS_0$ и $\exists AWS_1 \in AWS^*, AWS_1 \neq AWS_0$ такая, что $AWS'+AWS_1 = AWS_1+AWS'=AWS_0$. По определению $AWS' + AWS = (A' \cup A_1, V' \cup V_1, dom' \cup dom_1, cod' \cup cod_1)$.

Одно из множеств A', V', dom', cod' не равно пустому множеству и одно из множеств A, V, dom, cod не равно пустому множеству. Отсюда следует, что $\forall AWS', AWS_1$, не равных AWS_0 , $AWS_1 + AWS' \neq AWS_0$. Значит, получено противоречие – утверждение доказано.

Временные оценки параллельной композиции временных волновых систем

Пусть

$$AWS = (V, A, dom, cod, \tau, \bar{\tau}, t, \bar{t}),$$

$$AWS' = (V', A', dom', cod', \tau', \bar{\tau}', t', \bar{t}'),$$

тогда $AWS + AWS' = AWS_+$, в случае, если $A \cap A' = \emptyset, V \cap V' = \emptyset$. $AWS_+ = (A \cup A', V \cup V', dom \cup dom', cod \cup cod')$.

Предложение 1

$$\left[\sum_{v \in V} t(v) + \sum_{v \in V'} t'(v) \right] + \left[|A|(\tau + \bar{\tau}) + |A'|(\tau' + \bar{\tau}') \right] \geq T_{AWS_+} \geq \min \left[d \left(\max_{l \in Trace_{AWS}}(l) \right), d \left(\max_{l \in Trace_{AWS'}}(l) \right) \right].$$

Доказательство:

Запишем в более сжатой форме формулировку предложения $T_{AWS}^{\max} + T_{AWS'}^{\max} \geq T_{AWS_+} \geq \min(T_{AWS_+}^{\min}, T_{AWS'}^{\min})$, ясно, что параллельная композиция двух волновых систем не может функционировать быстрее, чем функционирует самая медленная ее составляющая, и медленнее, чем суммарное время, затраченное на функционирование каждой волновой системы в отдельности.

Предложение 1 допускает обобщение для семейства гибридных временных волновых систем.

Теорема 1. Пусть $AWS_+ = \sum_i AWS_i$, тогда справедливо $\sum_i T_{AWS_i}^{\max} \geq T_{AWS_+} \geq \min_i (T_{AWS_i}^{\min})$.

Доказательство:

Для случая двух временных волновых систем утверждение теоремы следует из предложения 1. Для произвольного количества временных волновых систем доказательство может быть получено по индукции.

Приведенная теорема позволяет получать априорные оценки времени функционирования временной волновой системы полученной в результате параллельной композиции произвольного числа взаимодействующих вычислительных процессов (узлов), если заданы оценки каждой составляющей.

Отметим, что параллельная композиция на множестве временных волновых систем – конструкция общая, что позволяет находить априорную верхнюю и нижнюю оценки функционирования результирующей временной волновой системы, даже в случае, когда исходные временные волновые системы описывали различные вычислительные процессы в различных вычислительных средах.

Последовательная композиция волновых систем

Пусть $AWS = (A, V, dom, cod)$, $AWS' = (A', V', dom', cod')$, $A \cap A' = V \cap V' = dom \cap dom' = cod \cap cod' = \emptyset$, $V = V_{in} \cup V_f \cup V_{out}$, $V' = V_{in'} \cup V_f' \cup V_{out'}$.

И пусть задана $f: V_{out} \rightarrow V_{in'}$ – биективное отображение.

Тогда определим операцию последовательной композиции на множестве волновых систем следующим образом, см. рис. 2:

$AWS \rightarrow AWS' = AWS^0$, $AWS^0 = (A^0, V^0, dom^0, cod^0)$, $V^0 = V \cup V'$, $A^0 = A \cup A' \cup A_\alpha$, $cod^0 = cod \cup cod' \cup cod_\alpha$, $dom^0 = dom \cup dom' \cup dom_\alpha$, $|A_\alpha| = |V_{out}|$ и для $\forall v \in V_{out} \exists a \in A_\alpha$ такая, что $dom^0(a) = v$, и эти стрелки образуют dom_α , $\forall a \in A_\alpha cod^0(a) = f(dom^0(a))$.

Утверждение 5. Операция $\rightarrow$ ассоциативна

$$(AWS \rightarrow AWS') \rightarrow AWS'' = AWS \rightarrow (AWS' \rightarrow AWS'').$$

Доказательство: следует непосредственно из определения.

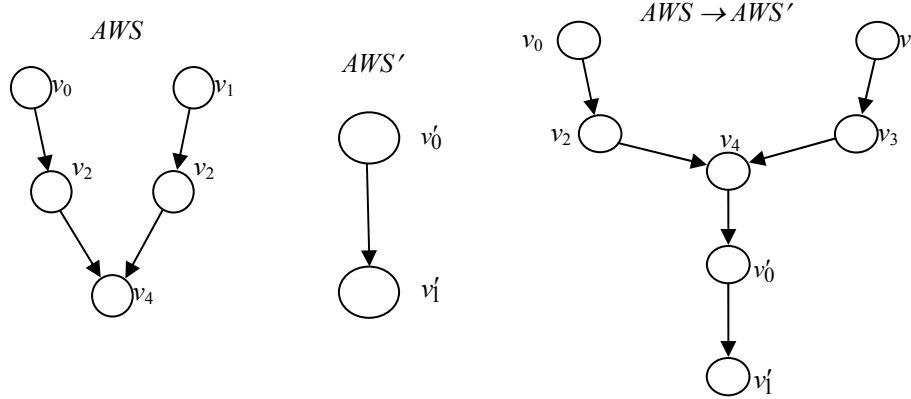


Рис. 2. Пример последовательной композиции двух волновых систем

Утверждение 6. Операция $\rightarrow$ не коммутативна.

Доказательство: существование биекции между V_{out} и V_{in} в общем случае не влечёт существования биекции между V_{in} и V_{out} . #.

Утверждение 7. Пара $(AWS^*, \rightarrow)$ – полугруппа.

Доказательство: по утверждению 5 операция $\rightarrow$ ассоциативна и $\forall AWS$ и $AWS', AWS \rightarrow AWS' \in AWS^*$.

Утверждение 8. Пара $(AWS^*, \rightarrow)$ – не моноид.

Доказательство: аналогично доказательству утверждения 4.

Последовательная композиция волновых систем определяет новую волновую систему, которая функционирует подобно первой, а после ее выполнения – как вторая, причем данные с выхода первой передаются на вход второй.

Временные оценки последовательной композиции гибридных временных волновых систем

Пусть заданы две гибридные временные волновые системы:

$$AWS = (V, A, dom, cod, \tau, \bar{\tau}, t),$$

$$AWS' = (V', A', dom', cod', \tau', \bar{\tau}', t'),$$

тогда $AWS \rightarrow AWS' = AWS^0$, а для A_α время посылки данных равно a , приема b , тогда справедливо следующее

Предложение 2

$$\left[\sum_{v \in V} t(v) + \sum_{v \in V'} t'(v) \right] + \left[|A|(\tau + \bar{\tau}) + |A'|(\tau' + \bar{\tau}') \right] + |V_{out}|(a+b) \geq T_{AWS^0} \geq d\left(\max_{l \in Trace_{AWS}}(l)\right) + d\left(\max_{l \in Trace_{AWS'}}(l)\right) + (a+b).$$

Доказательство:

Запишем в более сжатой форме формулировку предложения

$T_{AWS}^{\max} + T_{AWS'}^{\max} + |V_{out}|(a+b) \geq T_{AWS^0} \geq T_{AWS^0}^{\min} + T_{AWS}^{\min} + (a+b)$, очевидно, что последовательная композиция двух гибридных временных волновых систем не может функционировать быстрее, чем сумма минимальных времен функционирования каждой из них, учитывая затраты на пересылку пусть даже одного экземпляра данных между составляющими композиции. Также ясно, что время функционирования этой композиции не превзойдет суммарное время, затраченное на функционирование каждой гибридной временной волновой системы в отдельности и пересылки всех экземпляров данных, между выходными вершинами первой волновой системы и входными вершинами второй.

Предложение 2 допускает обобщение для семейства гибридных временных волновых систем.

Теорема 2. Пусть $AWS^0 = AWS_1 \rightarrow AWS_2 \rightarrow \dots \rightarrow AWS_n$, для $A_{1\alpha}$ время посылки данных равно a_1 , приема b_1 , для $A_{2\alpha}$ время посылки данных равно a_2 , приема b_2 и т.д., тогда справедливо

$$\sum_i (|V_{out}|(a_i + b_i) + T_{AWS_i}^{\max}) \geq T_{AWS^0} \geq \sum_i (T_{AWS_i}^{\min} + a_i + b_i).$$

Доказательство:

Для случая двух гибридных временных волновых систем утверждение теоремы следует из предложения 2. Для произвольного количества волновых систем доказательство может быть получено по индукции.

Приведенная теорема позволяет получать априорные оценки времени функционирования гибридной временной волновой системы, полученной в результате последовательной композиции произвольного числа взаимодействующих вычислительных систем, выполняющих некоторые вычисления параллельно, если заданы оценки каждой составляющей.

Причем так же, как и для параллельной композиции, не делается никаких предположений относительно состава вычислительных сред, которые были описаны при помощи исходных временных волновых систем.

Методика расчета времени, необходимого на перебор

Рассмотрим классический пример распределенного перебора ключей из множества X . Пусть мощность множества X кратна 4. Пусть процесс шифрования исходного сообщения размером 10 бит состоял в последовательном применении алгоритма Base64, затем проводилось гаммирование по ключу из множества X , далее выполнялся циклический сдвиг каждого разряда сообщения на 4 бита влево.

Пусть у нас имеется гетерогенная (неоднородная) вычислительная система с 24 вычислительными узлами, для данной вычислительной системы на прием данных одним вычислительным узлом тратится 1 с, на посылку – 2 с. Пусть специализированные узлы способны сдвигать некоторую последовательность на 1 бит вправо за 1 такт, другие могут выполнять сложение по модулю 2 последовательности из 10 бит за 1 такт, третьи – выполнять дешифрование по алгоритму Base64 последовательности из 10 бит за 1 такт. Пусть каждый такт каждого вычислительного узла составляет 1 с.

Рассмотрим временную волновую систему AWS (рис. 3), вершина которой выполняет сдвиг вправо на 1 бит исходной последовательности, множество ее ребер пусто, время исполнения операции в вершине – 1 такт, $\bar{\tau}=2$ и $\tau=1$.

Рассмотрим временную волновую систему AWS' (рис. 4), вершина которой выполняет сложение по модулю 2 последовательности из 10 бит, множество ее ребер пусто, время исполнения операции в вершине – 1 такт, $\bar{\tau}=2$ и $\tau=1$.

Рассмотрим временную волновую систему AWS_1 (рис. 5), вершина которой выполняет дешифрование последовательности из 10 бит по алгоритму Base64, множество ее ребер пусто, время исполнения операции в вершине – 1 такт, $\bar{\tau}=2$ и $\tau=1$.

AWS



Рис. 3. Временная волновая система для сдвига вправо на 1 бит

AWS'



Рис. 4. Временная волновая система для сложения по модулю 2

AWS_1



Рис. 5. Временная волновая система для сложения по модулю 2

Используя введенную операцию последовательной композиции, можно получить новую временную волновую систему, которая будет соответствовать сдвигу вправо на четыре разряда:

$$AWS^0 = AWS \rightarrow AWS \rightarrow AWS \rightarrow AWS.$$

По теореме 2 для последовательной композиции временных волновых систем получим:

$$\begin{aligned} \sum_i (|V_{out}|(a_i + b_i) + T_{AWS_i}^{\max}) &\geq T_{AWS_0} \geq \sum_i (T_{AWS_i}^{\min} + a_i + b_i), \\ \sum_i (1 * (\tau + \bar{\tau}) + 1) &\geq T_{AWS_0} \geq \sum_i (1 + \tau + \bar{\tau}), \\ 3 * 4 &\geq T_{AWS_0} \geq 3 * 4, \\ T_{AWS_0} &= 12. \end{aligned}$$

Далее рассмотрим последовательную композицию временной волновой системы, соответствующей сдвигу на 4 разряда вправо, затем выполнению гаммирования по ключу из множества X и выполнению дешифрования по алгоритму Base64 – $AWS^1 = AWS_0 \rightarrow AWS' \rightarrow AWS_1$.

По теореме 2 для последовательной композиции временных волновых систем получим:

$$\begin{aligned}\sum_i (|V_{i_{out}}| (a_i + b_i) + T_{AWS_i}^{\max}) &\geq T_{AWS^1} \geq \sum_i (T_{AWS_i}^{\min} + a_i + b_i), \\ \sum_i (1 * (\tau + \bar{\tau}) + 12) &\geq T_{AWS^1} \geq \sum_i (1 + \tau + \bar{\tau}), \\ 2 * 15 &\geq T_{AWS^1} \geq 2 * 4, \\ 30 &\geq T_{AWS^1} \geq 8.\end{aligned}$$

Отметим, что время, затрачиваемое на выполнение вычислений данной временной волновой системой, равно 20 с, но теорему 2 возможно применять и в случаях, когда время передачи данных между вычислительными узлами различно.

При функционировании временной волновой системы были задействованы 6 вычислительных узлов рассматриваемой нами вычислительной системы – четыре выполняют сдвиг, один – гаммирование по ключу, последний – дешифрование по алгоритму Base64.

Далее рассмотрим параллельную композицию четырех временных волновых систем AWS^1 см (рис. 6), они осуществляют схожие действия, но с различными ключами из множества X :

$$AWS^2 = AWS^1 + AWS^1 + AWS^1 + AWS^1.$$

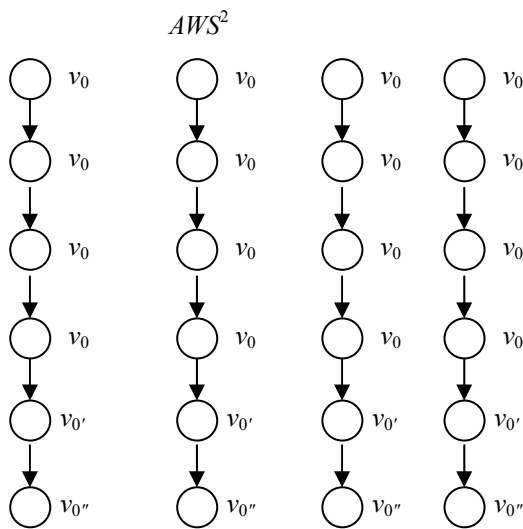


Рис. 6. Временная волновая система для сдвига вправо на 1 бит

По теореме 1 для параллельной композиции временных волновых систем получим:

$$\begin{aligned}\sum_i T_{AWS_i}^{\max} &\geq T_{AWS^2} \geq \min_i (T_{AWS_i}^{\min}), \\ 4 * 30 &\geq T_{AWS^2} \geq 8, \\ 120 &\geq T_{AWS^2} \geq 8.\end{aligned}$$

Отметим, что время, затрачиваемое на выполнение вычислений данной временной волновой системой, равно 20 в силу того, что все временные волновые системы, вошедшие в параллельную композицию, функционируют независимо и каждая вершина соответствует отдельному вычислительному узлу. Верхняя и нижняя границы времени, необходимого для перебора всех ключей в рассматриваемой вычислительной системе определяются соотношением

$$\frac{|X|}{4} 120 \geq T_{AWS^2} \geq \frac{|X|}{4} 8.$$

Заключение

В данной работе рассмотрен метод получения априорной верхней и нижней оценок времени проведения распределенного перебора в гетерогенных системах, построенных как последовательная и параллельная композиция более простых неоднородных или однородных вычислительных систем, на основе временных волновых систем. Моделирование задач распределенного перебора с использованием временных волновых систем дает возможность оценить время, которое будет потрачено на поиск решения, а введенные операции позволяют на основе волновых систем, описывающих некоторые простые стадии поиска решения, исполняемые в некоторой неоднородной среде, получать укрупненную модель и на основе времени функционирования каждой стадии получать время, которое будет затрачено на весь процесс поиска.

Литература

1. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.
2. Топорков В.В. Модели распределенных вычислений. – М.: Физматлит, 2004. – 320 с.
3. Трещёв И.А. Математическое моделирование волновых систем // XXXII Дальневосточная математическая школа-семинар им. академика Е.В. Золотова. – Владивосток: Дальнаука, 2007. – С. 101–102.

4. Трещев И.А. Математическая модель гибридной временной волновой системы // Системы управления и информационные технологии. – 2007. – № 4(30). – С. 19–21.

Трещев Иван Андреевич

Канд. техн. наук, доцент, зав. каф. «Информационная безопасность автоматизированных систем»

Комсомольского-на-Амуре государственного технического университета

Тел.: 8 (4217) 54-68-54

Эл. почта: kalkt@yandex.ru

Treshchov I.A.

Evaluation of time-cost for implementation of distributed brute force attack in heterogeneous systems using time wave systems

In this work the method of reception of aprioristic top and bottom estimations of time expenses for realization of distributed brute force attack in heterogeneous systems using time wave systems are considered. Time estimations for various variants of construction of heterogeneous systems are shown.

Keywords: distributed brute force attack, time-consuming estimate.
